IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. THOMAS G. DUNCAN, Defendant.	3:15-cr-00414-JO OPINION & ORDER

JONES, District Judge,

This is one of many cases across the country originating from a search warrant issued by a magistrate judge in the Eastern District of Virginia. The matter is before the court on two motions by defendant to suppress evidence derived from that warrant. [Doc # 37, Doc # 47] The court has considered the briefs submitted by the parties, and the outstanding arguments presented by counsel for both parties at the hearing held on November 16, 2016. Because defendants across the country have challenged the same Virginia search warrant, over two dozen district courts have weighed in on the issues raised here, and the court has considered those decisions, as well.

Defendant is charged with several counts of producing and possessing child pornography and allowing a child to be used in the production of child pornography, in violation of 18 U.S.C. §§ 2251, 2252A. He seeks to suppress numerous images and videos depicting child pornography found

on his computers and other digital storage media seized at his residence. He also seeks to suppress statements he made in an interview conducted while his residence was being searched, including admissions that he sexually abused his fiancée's daughter and produced child pornography of her beginning when she was 12 years old. He does not challenge directly the search warrant issued in the District of Oregon for the search of his residence. He contends, however, that the Oregon search warrant was founded entirely on information improperly obtained through the warrant issued in the Eastern District of Virginia.

The Virginia warrant authorized the FBI to deploy a network investigative technique ("NIT") on a child pornography website. Individuals across the country who downloaded child pornography from the website also downloaded the NIT onto their computers. The NIT then caused those computers to transmit identifying information back to a government controlled computer.

In his first motion [Doc # 37], defendant contends that the Virginia warrant authorizing the NIT was void *ab initio* because the magistrate judge had no authority to issue it under 28 U.S.C. § 636(a). He next contends the warrant violated Federal Rule of Criminal Procedure 41, because it authorized searches of computers outside the geographical boundaries of the Eastern District of Virginia. In his second motion [Doc # 47], defendant contends the Virginia NIT warrant violated the particularity requirement of the Fourth Amendment because it did not identify specific persons or places to be searched. Defendant seeks a single remedy, *viz* suppression of all the evidence derived from the NIT warrant.

BACKGROUND

Other district courts have provided detailed descriptions of the technological background in which the issues in this case arose. *See e.g. United States v. Knowles*, 2016 WL 6952109 (D.S.C.

Sept. 14, 2016). That background is further described in the Affidavit of Special Agent Douglas Mcfarlane in support of the NIT search warrant, which defendant does not challenge for the accuracy of its description of these background facts. [Doc # 44-3] A brief summary will suffice here.

A website known as "Playpen" operated as a hidden service on a network of servers called "Tor" which provides for anonymous internet communications. Playpen was dedicated to the global advertisement and distribution of child pornography and provided a forum for the discussion and depiction of the sexual abuse of children. The website offered image and video hosting which enabled producers and traders of child pornography to anonymously upload images and videos for other anonymous users to view. Thousands of unique anonymous users utilized the Tor network to visit the Playpen website. When the FBI shut the Playpen website down in March 2015, it had over two hundred thousand registered member accounts and over 1500 daily visitors.

In February 2015 the FBI obtained a copy of the Playpen website and stored it on a government controlled computer server in Newington, Virginia. The FBI assumed control of the Playpen website and permitted it to continue operating temporarily. In the Eastern District of Virginia, Special Agent Mcfarlane applied for and received a search warrant authorizing the use of a NIT to overcome the anonymity provided by the Tor network. The warrant authorized the FBI to deploy the NIT on the Playpen website. In essence, the NIT amounted to instructions in computer code that attached to or augmented illicit content. A person accessing illicit content on the Playpen website would unknowingly also download the NIT, which would then instruct the downloading computer to transmit information back to a government controlled computer. The information included the IP address and other information that would help the FBI to determine the location and user of the computer. The FBI configured the NIT to activate only after an individual logged into

the Playpen website with a registered member account username and password and then accessed a post containing child pornography. The NIT activation occurred invisibly and instantaneously without the user's knowledge.

The FBI allowed the Playpen website to continue operating for two weeks during the NIT deployment. During that period, information obtained by the NIT deployment enabled the identification of at least 137 persons who were charged with crimes, including 35 alleged child molesters and 17 alleged producers of child pornography. At least 26 child victims were identified. *United States v. Michaud*, Crim. No. 15-5351 (W.D. Wa. Jan. 8, 2016) Dkt.109. The information obtained by the FBI during that period included the IP address associated with the computer of a registered Playpen member with the user name "danigirl12." The IP address was tracked back to the residence where defendant lived with his fiancée and her two daughters in the District of Oregon. The FBI later obtained an Oregon search warrant for the residence. When the search was executed, the FBI obtained the evidence defendant now seeks to suppress.

DISCUSSION

I. Potential Violations

The many cases originating from the Virginia NIT warrant illustrate the difficulties involved in applying traditional Fourth Amendment protections in the context of rapidly advancing computer network technology. Reasonable jurists have reached different conclusions on issues including whether the NIT deployment amounted to a search implicating the Fourth Amendment, whether the NIT deployment fell within any of the subcategories of Rule 41, and whether the warrant identified with sufficient particularity the persons and places to be searched. Those issues are adequately framed by the existing decisions and additional analysis here will serve little purpose.

First, the court is unpersuaded by the government's argument that there was no search because defendant lacked a reasonable expectation of privacy in his IP address. Some courts looking at this fact pattern have found no expectation of privacy. *See e.g. United States v. Jean*, 2016 WL 4771096 at *9 (W.D. Ark. Sept 13, 2016); *United States v. Acevedo-Lumus*, 2016 WL 4208436 at *6 (C.D. Cal. Aug 8 2016). For the purposes of resolving this motion, however, I assume that defendant had sufficient expectation of privacy in information stored on his computer inside his residence to implicate Fourth Amendment protections.

Next, the court rejects defendant's argument that the NIT warrant was void *ab initio* because the magistrate judge had no authority under 28 U.S.C. §636(a). Without question, the magistrate judge had authority to issue warrants in the Eastern District of Virginia to search computers within that district. Although there are reasonable questions whether the NIT deployment involved a search outside that district and whether such action was authorized by the warrant, the warrant itself was not wholly without statutory authority, so it was not void when it was issued. *See e.g. United States v. Anzalone*, 2016 WL 5339723, *11(D. Mass. Sept 9, 2016). Even assuming defendant is correct, however, such a defect does not automatically trigger suppression under the exclusionary rule. *Herring v. United States*, 555 U.S. 135, 146 (2009); *U. S. v. Leon*, 468 U.S. 897, 906 (1984).

Turning to the potential rule violation, the court notes that there are cogent reasons by which several courts have found the NIT was a tracking device authorized under Rule 41(b)(4) or was analogous to a tracking device and should be permitted under a flexible application of Rule 41(b)(4). *See e.g. United States v. Darby*, 2016 WL 3189703, *12 (E.D. Va. June 3, 2016). For the purposes of resolving this motion, however, I find the NIT was similar to, but not technically equivalent to a tracking device. I assume, that the warrant technically violated the letter, but not the spirit of Rule

41(b). *See e.g. United States v. Michaud*, 2016 WL 337263, *6 (W.D. Wa. Jan. 28, 2016). Notably, the Supreme Court has now recommended a modification to Rule 41 that would explicitly authorize warrants like the NIT warrant challenged here. *Acevedo-Lemus*, 2016 WL 4208436 at *8.

Regarding the Fourth Amendment issue, I find the warrant was sufficiently specific to satisfy the particularity requirement of the Fourth Amendment. The warrant directed the deployment of the NIT only to the computers of individuals who knowingly and intentionally sought out and downloaded illicit content from the Playpen website. The warrant made clear to the extent possible in the context of the anonymity provided by the Tor network, what computers could be searched and what specific limited information could be retrieved. *United States v. Turner*, 770 F.2d 1508, 1510 (9th Cir. 1985); *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009). Again, even assuming defendant is correct on this issue, the defect would not automatically trigger suppression. *Herring*, 555 U.S. at 146; *Leon*, 468 U.S. at 146.

II. The Exclusionary Rule

Defendant seeks suppression of evidence under the exclusionary rule. The exclusionary rule operates as "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a constitutional right of the party aggrieved." *U. S. v. Leon*, 468 U.S. at 906 quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974). It can only be applied to the extent that the exclusion of evidence obtained by culpable police conduct will have an appreciable deterrent effect on future unlawful police conduct. *Herring*, 555 U.S. at 137; *U.S. v. Leon*, 468 U.S. at 918.

This limitation on the exclusionary rule applies to violations of Rule 41 because the Federal Rules of Criminal procedure do not expand the exclusionary rule. *United States v. Willimason*, 439

F.3d 1125, 1132 (9th Cir. 2006). In the Ninth Circuit, evidence may be suppressed for a violation of Rule 41(b) if the violation results in prejudice to the defendant, where prejudice means that a search could not have occurred without a violation of the rule, or if law enforcement personnel intentionally and deliberately disregarded the rule. *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005). Here, defendant did not suffer prejudice in the sense contemplated in *Weiland*. Law enforcement could have obtained warrants in each of the 94 judicial districts across the country without violating defendant's asserted interpretation of Rule 41(b). The FBI reasonably did not do so, given the expense and time that would be required to accomplish such a feat.

Here, FBI agents were diligent in their investigation of the Playpen website and entirely truthful with the magistrate judge. Special Agent Mcfarlane provided a detailed description of the Tor network and how it operated to hide the Playpen website, how the NIT deployment functioned, which computers would be targeted, and what information would be obtained from them. He told the magistrate judge that computers in unknown locations, including some outside the Eastern District of Virginia, would download the NIT. He asserted that the NIT operated like a tracking device authorized under Rule 41(b)(4), and the magistrate judge agreed.

Various courts addressing this issue are split and appellate courts may ultimately conclude that the magistrate judge interpreted Rule 41 incorrectly, but this does not suggest that the FBI attempted to mislead the magistrate judge or intentionally disregarded the rule. In sum, the individual FBI agents and the national agency as a whole acted in good faith.

Therefore, in the absence of any misconduct by the FBI, suppression of the evidence in this case would have no deterrent effect on future police conduct. Accordingly, defendant's motions must be denied. *Herring*, 555 U.S. at 137; *U.S. v. Leon*, 468 U.S. at 918.

CONCLUSION

For the foregoing reasons, defendant's two motion to suppress [Doc # 37, Doc # 47] are DENIED.

IT IS SO ORDERED.

DATED this 6 day of December, 2016.

Robert E. Jones
United States District Judge